

QUADRATIC CONGRUENCES

by

MARY JEANE STARKEY MCGUIRE

B. A., Kansas State University, 1961

---

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF ART

Department of Mathematics

KANSAS STATE UNIVERSITY  
Manhattan, Kansas

1963

Approved by:

Richard Yates  
Major Professor

1.D  
2668  
R4  
1963  
01147  
C.2

TABLE OF CONTENTS

	Page
INTRODUCTION . . . . .	1
GENERAL CONGRUENCES OF DEGREE $n$ . . . . .	2
QUADRATIC CONGRUENCES . . . . .	9
THE LEGENDRE SYMBOL . . . . .	12
THE LAW OF QUADRATIC RECIPROCITY . . . . .	20
THE JACOBI SYMBOL . . . . .	23
THE GENERALIZED LAW OF QUADRATIC RECIPROCITY . . . . .	26
CONCLUSION . . . . .	29
ACKNOWLEDGMENT . . . . .	32
BIBLIOGRAPHY . . . . .	33

## INTRODUCTION

The purpose of this paper is to investigate the problem of solving quadratic congruences. For a given quadratic congruence this can be accomplished through repeated substitution of integers into the congruence to find those residue classes which are solutions. In general, however, this method of trial substitution is of prohibitive length. Instead, the given congruence may be reduced to several congruences which in turn are solved by a more feasible number of trials. Moreover, determining the number of solutions that exist can greatly reduce the number of trials needed. Ascertaining that no solutions exist obviously eliminates the necessity of repeated trials entirely.

This question of the existence of solutions will also be considered because of its fundamental importance to the theory of quadratic congruences. Initially quadratic residues will be defined, followed by the introduction of the Legendre symbol. Theorems regarding the Legendre symbol then culminate in the law of quadratic reciprocity, fundamental to the theory of quadratic residues. Finally, the generalized symbol of Jacobi will be introduced as a tool in dealing with Legendre's symbol. This existence theory will then be applied to the general question of solving quadratic congruences to be illustrated in a final example.

GENERAL CONGRUENCES OF DEGREE  $n$ 

The definitions of congruence and of residue class must be introduced as a basis for any comments on quadratic congruences. The relation of congruence is merely a statement about the divisibility of the difference of two numbers.<sup>1</sup> If  $a-b$  is divisible by a non-zero integer  $m$ , then  $a$  is congruent to  $b$  modulo  $m$ , written  $a \equiv b \pmod{m}$ . If  $a-b$  is not divisible by  $m$ , then  $a$  is incongruent to  $b$  modulo  $m$ , written  $a \not\equiv b \pmod{m}$ . Since  $a-b$  is divisible by  $m$  if, and only if,  $a-b$  is divisible by  $-m$ , discussion will be limited to moduli that are positive integers. Congruence is an equivalence relation with equivalence classes called residue classes. Thus, for any integer  $a$ , the residue class  $R_a$  is the subset of all integers  $b$  such that  $b \equiv a \pmod{m}$ . It follows that any two integers of the same residue class are congruent to each other and that each integer belongs to one and only one distinct residue class modulo  $m$ . The congruence relation modulo  $m$  separates the set of all integers into  $m$  residue classes, denoted by  $R_0, R_1, \dots, R_{m-1}$ , with representatives  $0, 1, \dots, m-1$ , respectively.

Deriving congruences from the congruence relation follows as the analogue to deriving equations from the relation of equality. If  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ ,  $n \geq 1$ , is a polynomial with integral coefficients and  $a_0 \not\equiv 0 \pmod{m}$ , then  $f(x) \equiv 0 \pmod{m}$  is a congruence of degree  $n$ . If  $u$  is an integer such that  $f(u) \equiv 0 \pmod{m}$ , then  $u$

---

<sup>1</sup>Throughout this paper "number" or "integer" will be understood to mean rational integer.

satisfies the congruence  $f(x) \equiv 0 \pmod{m}$ . However, the nature of a modulo system dictates that if  $f(x) \equiv 0 \pmod{m}$  is satisfied by  $u$ , it is satisfied by an infinite number of integers--all those congruent modulo  $m$  to  $u$ . This is shown in the theorem that follows.

Theorem 1. For any polynomial  $f(x)$  with integral coefficients such

that  $f(x) = c_0 + c_1x + \dots + c_nx^n = \sum_{v=0}^n c_vx^v$  ( $n \geq 0$ ), if  $a \equiv b \pmod{m}$ ,

then  $f(a) \equiv f(b) \pmod{m}$ .

Proof. Since two congruences with the same moduli may be multiplied member by member and may be added member by member, congruences (1) result from the given  $a \equiv b \pmod{m}$ , where it is understood that  $c_v \equiv c_v \pmod{m}$  for all  $0 \leq v \leq n$ .

$$a^v \equiv b^v \pmod{m}, \quad 0 \leq v \leq n$$

$$(1) \quad c_v a^v \equiv c_v b^v \pmod{m}, \quad 0 \leq v \leq n$$

$$\sum_{v=0}^n c_v a^v \equiv \sum_{v=0}^n c_v b^v \pmod{m}$$

that is,  $f(a) \equiv f(b) \pmod{m}$ .

It follows from this theorem that the integers which satisfy the congruence  $f(x) \equiv 0 \pmod{m}$  fall into residue classes modulo  $m$ . Therefore, the number of solutions of  $f(x) \equiv 0 \pmod{m}$  is defined to be the number of residue classes all of whose members satisfy  $f(x) \equiv 0 \pmod{m}$ . Since there are just  $m$  residue classes modulo  $m$ , there can never be more than  $m$  solutions of a congruence modulo  $m$ . Furthermore, Lagrange's theorem states that for a prime modulus the number of solutions is never

greater than the degree of the congruence.<sup>2</sup>

Since Lagrange's theorem and many theorems of specific importance to the theory of quadratic congruences apply only to congruences with prime moduli,<sup>3</sup> to express any congruence modulo  $m$  in terms of congruences modulo  $p$  is the initial problem in establishing a general method for solving congruences. This process of reduction will be considered for the general congruence of degree  $n$ . A quadratic congruence will then be discussed as the specific case in which  $n$  equals two.

The fundamental theorem of arithmetic allows the first step in reducing the general congruence. Except for associated primes and the order of the factors, a composite integer can be factored uniquely into powers of distinct primes; that is  $m = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r}$ . This form of the integer  $m$  is called its canonical decomposition. Thus a composite modulus may be replaced by its canonical decomposition, and the following theorem for the number of solutions of a congruence with composite modulus is developed.

Theorem 2. If  $m > 1$ , and its canonical decomposition is

$$(2) \quad m = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r},$$

then the number of solutions of

$$(3) \quad f(x) \equiv 0 \pmod{m}$$

<sup>2</sup>For proof, see Elementary Theory of Numbers, Harriet Griffin, pp. 75-77.

<sup>3</sup>A prime modulus will be indicated by the letter  $p$  in contrast with the use of the letter  $m$  to indicate the general composite modulus.

is equal to the product of the numbers of solutions of the  $r$  congruences

$$(4) \quad f(x) \equiv 0 \pmod{p_i^{s_i}} \text{ for } i = 1, \dots, r.$$

Proof. Since a composite modulus may be factored into powers of distinct primes and these factors are relatively prime in pairs, a congruence (3) is equivalent to the system of simultaneous congruences (4), where the canonical decomposition of  $m$  is given by (2). Consequently, any solution of (3) must be congruent modulo  $p_1^{s_1}$  to some solution  $d_1$  of  $f(x) \equiv 0 \pmod{p_1^{s_1}}$ , congruent modulo  $p_2^{s_2}$  to some solution  $d_2$  of  $f(x) \equiv 0 \pmod{p_2^{s_2}}$ , and similarly congruent modulo  $p_i^{s_i}$  to some solution  $d_i$  of the corresponding congruence  $f(x) \equiv 0 \pmod{p_i^{s_i}}$  for  $i = 1, 2, \dots, r$ . Conversely, if arbitrarily chosen solutions of the congruences (4) are designated by  $d_1, d_2, \dots, d_r$ , then  $x$  may be determined by the simultaneous congruences

$$(5) \quad x \equiv d_i \pmod{p_i^{s_i}} \text{ for } i = 1, 2, \dots, r.$$

Solutions of this system of congruences may be found using the so-called Chinese method, or Chinese remainder theorem. Then each solution will be a solution of the congruence (3). To obtain all possible solutions of (3), one must choose all possible sets of values  $d_1, d_2, \dots, d_r$ , and for each corresponding system (5) obtain a value of  $x$  which will be a solution of (3), incongruent modulo  $m$  to every other value of  $x$  obtained. Hence, if  $N(m)$  denotes the number of distinct solutions of (3) and the notation is used similarly for each of the congruences (4), then

$$N(m) = N(p_1^{s_1})N(p_2^{s_2}) \dots N(p_r^{s_r}).$$

It is evident that if one of the congruences (4) fails to have a solution, there is no solution for (3). Furthermore, through the following theorem, solving a congruence of the form  $f(x) \equiv 0 \pmod{p^s}$  may be reduced to solving  $f(x) \equiv 0 \pmod{p^{s-1}}$ , which reduces by induction to solving  $f(x) \equiv 0 \pmod{p}$ .

Theorem 3. If  $s > 1$ , the solutions of

$$(6) \quad f(x) \equiv 0 \pmod{p^s},$$

where  $p$  is a prime, are determined by the solutions of

$$(7) \quad f(x) \equiv 0 \pmod{p^{s-1}}.$$

Proof. Every solution of (6) is congruent modulo  $p^{s-1}$  to some solution  $b$  of congruence (7) although there may be more solutions of (6) than of (7) because integers congruent modulo  $p^{s-1}$  may be incongruent modulo  $p^s$ . Solutions of (6) may be written in the form  $x = b + p^{s-1}t$ , where  $b$  has been found to be a solution of (7). Therefore, by Taylor's expansion,

$$f(x) = f(b) + p^{s-1}tf'(b) + p^{2s-2}t^2 \frac{f''(b)}{1 \cdot 2} + \dots. \text{ All terms begin-}$$

ning with the third are divisible by  $p^s$  since  $2s-2 \geq s$  if  $s > 1$  and  $\frac{f''(b)}{1 \cdot 2}$ ,

$$\frac{f'''(b)}{1 \cdot 2 \cdot 3}, \dots \text{ are integers. Hence, } f(x) \equiv f(b) + p^{s-1}tf'(b) \pmod{p^s}.$$

Since  $f(b) \equiv 0 \pmod{p^{s-1}}$ , there exists an integer  $Q$  such that

$f(b) = Qp^{s-1}$ . If  $f(x) \equiv 0 \pmod{p^s}$  is written  $f(b) + tp^{s-1}f'(b) \equiv 0 \pmod{p^s}$ , substituting for  $f(b)$  gives

$$(3) \quad Q + tf'(b) \equiv 0 \pmod{p}.$$

The following two cases result.

Case I: If  $f'(b)$  is not divisible by  $p$ , congruence (8) has a unique solution modulo  $p$ . Hence, a unique solution of (6) will correspond to each solution of (7).

Case II. If  $f'(b)$  is divisible by  $p$ , congruence (8) either has  $p$  solutions or is impossible. Hence, (6) has either  $p$  solutions or no solutions corresponding to each solution of (7).

The procedure defined in this theorem consists, then, of the following steps. First the congruence modulo  $p$  must be solved. Then solutions of  $f(x) \equiv 0 \pmod{p^2}$  corresponding to each solution of  $f(x) \equiv 0 \pmod{p}$  are obtained. This process is continued through successive powers of the prime modulus until all solutions have been found for the congruence modulo  $p^s$ . This procedure and that of theorem 2 are outlined in the following example.

Example 1. Find all solutions of the congruence

$$(9) \quad f(x) \equiv 0 \pmod{100}$$

with  $f(x) = x^3 + 3x^2 + x + 3$ . The canonical decomposition of 100 is  $100 = 2^2 \cdot 5^2$ . Thus (9) is equivalent to the system of simultaneous congruences

$$(10) \quad f(x) \equiv 0 \pmod{2^2}$$

$$(11) \quad f(x) \equiv 0 \pmod{5^2}.$$

Theorem 3 must be used to find the solutions of both congruences (10) and (11).

The solution of  $f(x) \equiv 0 \pmod{2}$  by trial substitution is 1.

Solving (10) involves the following:

$$b=1,$$

$$f(b)=3 \equiv 0 \pmod{2}, f(b)=1 \cdot 2, Q=4,$$

$$f'(b)=10.$$

Since 2 divides  $f'(b)$ , there will be two solutions of (10) corresponding to  $b=1$ . Congruence (8) becomes  $4+10t \equiv 0 \pmod{2}$ , which holds for all values of  $t$  in the modulo system. For  $t=0$ ,  $x=2t+b=1$ . For  $t=1$ ,  $x=2t+b=3$ . Therefore,  $f(x) \equiv 0 \pmod{4}$  has solutions 1 and 3. In this particular case one could have anticipated the solution  $x=1$  because  $f(1)$  is a multiple of 4 as well as a multiple of 2.

The solutions of  $f(x) \equiv 0 \pmod{5}$  are obtained by trial substitution; they are 2 and 3. Then, the determination of the solutions of (11) is broken into two parts.

Part I:  $b=2$

$$f(b)=25 \equiv 0 \pmod{5}, f(b)=Q \cdot 5, Q=5.$$

$$f'(b)=25.$$

Since 5 divides  $f'(b)$ , there will be five solutions of (11) corresponding to  $b=2$ . Congruence (8) becomes  $5+25t \equiv 0 \pmod{5}$ , which is satisfied by all values of  $t$  in the modulo system. For  $t=0$ ,  $x=5t+b=2$ . For  $t=1$ ,  $x=5t+2=7$ . For  $t=2$ ,  $x=5t+2=12$ . For  $t=3$ ,  $x=5t+2=17$ . For  $t=4$ ,  $x=5t+2=22$ . Therefore,  $f(x) \equiv 0 \pmod{25}$  has solutions 2, 7, 12, 17, and 22 corresponding to  $b=2$ .

Part II:  $b=3$ ,

$$f(b)=60 \equiv 0 \pmod{5}, f(b)=Q \cdot 5, Q=12,$$

$$f'(b)=46.$$

Since 5 does not divide  $f'(b)$ , there will be a unique solution of (11) corresponding to  $b=3$ . Congruence (8) becomes  $12+46t \equiv 0 \pmod{5}$ ,

which is satisfied by  $t=3$ . For  $t=3$ ,  $x=5t+b=18$ . Therefore,  $f(x) \equiv 0 \pmod{25}$  has the solution  $x=18$  corresponding to  $b=3$ .

Since there are two solutions of (10) and six solutions of (11), the congruence to be solved (9) will have twelve solutions, determined by twelve systems (5), each of which will be of the form  $x \equiv d_1 \pmod{4}$ ,  $x \equiv d_2 \pmod{25}$  for  $d_1$  and  $d_2$  ranging over all solutions of (10) and (11) respectively. Using the Chinese method, one obtains the following congruence to give all solutions of (9) for the twelve different sets of  $d_1$  and  $d_2$ :  $x \equiv 25d_1 + 76d_2 \pmod{100}$ . The final results are then tabulated as follows:

$d_1$	$d_2$	$x$
1	2	$25 + 152 = 177 \equiv 77 \pmod{100}$
1	7	$25 + 532 = 557 \equiv 57 \pmod{100}$
1	12	$25 + 912 = 937 \equiv 37 \pmod{100}$
1	17	$25 + 1292 = 1317 \equiv 17 \pmod{100}$
1	18	$25 + 1368 = 1393 \equiv 93 \pmod{100}$
1	22	$25 + 1672 = 1697 \equiv 97 \pmod{100}$
3	2	$75 + 152 = 227 \equiv 27 \pmod{100}$
3	7	$75 + 532 = 607 \equiv 7 \pmod{100}$
3	12	$75 + 912 = 987 \equiv 87 \pmod{100}$
3	17	$75 + 1292 = 1367 \equiv 67 \pmod{100}$
3	18	$75 + 1368 = 1443 \equiv 43 \pmod{100}$
3	22	$75 + 1672 = 1747 \equiv 47 \pmod{100}$

Therefore, the solutions of  $f(x) \equiv 0 \pmod{100}$  are 7, 17, 27, 37, 43, 47, 57, 67, 77, 87, 93, 97.

#### QUADRATIC CONGRUENCES

From the preceding consideration of the general congruence of degree  $n$  results have been obtained which may now be applied to the

proposed problem, that of solving the general quadratic congruence

$$(12) \quad ax^2+bx+c \equiv 0(\text{mod } m), \quad a \not\equiv 0(\text{mod } m).$$

Congruence (12) with  $a \equiv 1$  and  $b \equiv 0$  is defined to be the binomial quadratic congruence. Since (12) is clearly the general congruence of degree  $n$  with  $n=2$ , theorems 2 and 3 imply that solving (12) depends upon solving congruences of the form

$$(13) \quad ax^2+bx+c \equiv 0(\text{mod } p).$$

The following theorem simplifies the solving the general quadratic congruence still further.

Theorem 4. If  $f(x)=ax^2+bx+c$  and  $a \not\equiv 0(\text{mod } p)$  for an odd prime  $p$ , then the solutions of  $f(x) \equiv 0(\text{mod } p)$  are determined by the solutions of the pair of congruences  $u^2 \equiv b^2-4ac \pmod{p}$  and  $2ax+b \equiv u(\text{mod } p)$ .

Proof. Since  $p$  is an odd prime and  $a \not\equiv 0(\text{mod } p)$ ,  $(4a,p)=1$ .

Multiplying  $f(x) \equiv 0(\text{mod } p)$  by  $4a$  and adding  $b^2-4ac$  yields

$$(2ax+b)^2 \equiv b^2-4ac \pmod{p}. \quad \text{Hence, } x_1 \text{ is a solution of } f(x) \equiv 0(\text{mod } p)$$

if, and only if,  $2ax_1+b \equiv u(\text{mod } p)$ , in which  $u$  is a solution of

$u^2 \equiv b^2-4ac \pmod{p}$ . Furthermore, since  $(2a,p)=1$ , for each solution  $u$  there is one, and only one,  $x$  modulo  $p$  such that  $2ax+b \equiv u(\text{mod } p)$ ; and different  $u$  modulo  $p$  will yield different  $x$  modulo  $p$ .

Finally then, solving a general quadratic congruence reduces to solving linear congruences and binomial quadratic congruences in which the moduli are primes. The number of trial substitutions

<sup>4</sup>Since the case for which  $p=2$  may be solved by trial substitution,  $p$  will be restricted to odd primes.

required to obtain all solutions is thus reduced. Since the solvability of the general quadratic congruence depends on the existence of solutions of all corresponding binomial quadratic congruences, determining that any one of them has no solution leads directly to the conclusion that no solution exists for the given congruence. For this reason, consideration of quadratic residues is pertinent.

The values of  $c \neq 0$  for which the congruence  $x^2 \equiv c \pmod{p}$  is solvable are called quadratic residues of the odd prime  $p$ . Quadratic non-residues are those values of  $c$  for which the congruence has no solution. This quality of being a quadratic residue or non-residue modulo  $p$  is called the quadratic character of  $c$  with respect to  $p$ . Determining the quadratic character of  $c$  is, therefore, equivalent to testing for the existence of solutions of  $x^2 \equiv c \pmod{p}$ . The following theorem resolves the question of the number of possible solutions.

Theorem 5. If  $c$  is a quadratic residue modulo  $p$ , then the congruence

$$(14) \quad x^2 \equiv c \pmod{p}$$

has two solutions.

Proof. By the definition of quadratic residue, if  $c$  is a quadratic residue, then (14) has at least one solution  $u \pmod{p}$ . Since  $(-u)^2 = u^2$ , the same congruence has a second solution,  $-u \pmod{p}$ . This second solution is different from the first since  $u \equiv -u \pmod{p}$  implies  $2u \equiv 0 \pmod{p}$  which is impossible because both 2 and  $u$  are relatively prime to  $p$ . By Lagrange's theorem the congruence of degree two has at most two solutions; hence, these two solutions,  $u$  and  $-u$ , exhaust all possible solutions of (14).

## THE LEGENDRE SYMBOL

Investigating the quadratic residues of odd primes leads to use of the following simplifying notation introduced by Legendre. The Legendre symbol  $(c/p)$ , where  $c$  is not divisible by the prime  $p$  is defined as follows:

$(c/p) = 1$  if  $c$  is a quadratic residue of  $p$ ,

$(c/p) = -1$  if  $c$  is a quadratic non-residue of  $p$ .

In order to define the symbol for every integer  $c$ , the following may be added:  $(c/p) = 0$  if  $p$  divides  $c$ . Then a concise expression denoting the number of solutions existent for any binary quadratic congruence follows from the extended definition of the Legendre symbol.

Theorem 6. The number of solutions of the congruence (14) for any  $c$  and any prime  $p$  is  $1 + (c/p)$ .

Proof. There are three cases to be considered.

Case I: If  $c$  is a quadratic residue of  $p$ ,  $1 + (c/p) = 1 + 1 = 2$ . This was proved in theorem 5 to be the number of solutions of the congruence (14) if  $c$  is a quadratic residue of  $p$ .

Case II: If  $p$  divides  $c$ , then  $c$  is a multiple of  $p$ . Thus,  $x^2$  must be a multiple of  $p$  which implies that  $x$  must be a multiple of  $p$  since  $p$  is a prime. Now all multiples of  $p$  belong to the same residue class modulo  $p$ . Hence, all possible values of  $x$  are in the same residue class modulo  $p$ ; and this residue class will be the only solution of the congruence (14). Then for case II,  $1 + (c/p) = 1 + 0 = 1$ , which is the number of existing solutions of (14).

Case III: If  $c$  is a quadratic non-residue of  $p$ , there are no solutions of the congruence (14). This is exactly the result,  $1 + (c/p) = 1 + (-1) = 0$ .

A fundamental tool in evaluating Legendre's symbol is Euler's criterion, which is stated here without proof. From it, for a given odd prime modulus, the quadratic character of any number can be determined.

Euler's criterion.<sup>5</sup> If  $p$  is an odd prime and  $p$  does not divide  $c$ , then  $c^{(p-1)/2} \equiv 1 \pmod{p}$  or  $c^{(p-1)/2} \equiv -1 \pmod{p}$  according as  $c$  is a quadratic residue or non-residue of  $p$ .

By Euler's criterion, Legendre's symbol is uniquely defined by the congruence

$$(15) \quad (c/p) \equiv c^{(p-1)/2} \pmod{p}.$$

Hence, certain properties which simplify the evaluation of Legendre's symbol may be proved. These are given in the following theorem.

Theorem 7. The Legendre symbol has the following properties:

- I.  $(cb/p) = (c/p)(b/p)$ .
- II. If  $c \equiv b \pmod{p}$ , then  $(c/p) = (b/p)$ .
- III. If  $p$  does not divide  $c$ ,  $(c^2/p) = 1$ .
- IV. If  $p$  does not divide  $b$ ,  $(cb^2/p) = (c/p)$ .
- V.  $(1/p) = 1$ .
- VI.  $(-1/p) = (-1)^{(p-1)/2}$ .

Proof. Each of the six properties must be considered separately.

Property I. From Euler's criterion,

$$(cb/p) \equiv (cb)^{(p-1)/2} \equiv c^{(p-1)/2} b^{(p-1)/2} \pmod{p}.$$

Hence,  $(cb/p) \equiv (c/p)(b/p) \pmod{p}$ . Since Legendre's symbol assumes

<sup>5</sup>For proof, see Elementary Number Theory, Edmund Landau, p. 54.

only the values of 0 and  $\pm 1$ , the following equality holds:

$(cb/p) = (c/p)(b/p)$ . Thus the product of two residues or two non-residues is a residue; the product of a residue and a non-residue is a non-residue. If  $p$  divides  $cb$ , both sides of the equality will obviously be zero since  $p$  will necessarily, then, divide  $c$  or  $b$ .

Property II. Since  $c \equiv b \pmod{p}$ ,  $c$  and  $b$  are members of the same residue class modulo  $p$ . The numbers of a particular residue class are either all solutions or all not solutions of a particular congruence. Thus  $c$  and  $b$  are of the same quadratic character; that is,  $(c/p) = (b/p)$ .

Property III. From property I,  $(c^2/p) = (c/p)(c/p)$ . Thus, since  $(c/p)$  is equal to  $\pm 1$ ,  $(c^2/p) = +1$ .

Property IV. From property I,  $(cb^2/p) = (c/p)(b^2/p)$ . From property III,  $(c/p)(b^2/p) = (c/p)(+1) = (c/p)$ .

Property V. Because 1 raised to the power of  $(p-1)/2$  will always equal 1, congruence (15) becomes for  $c = 1$ ,  $(1/p) = 1$ .

Property VI. If in (15)  $c = -1$ ,  $(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}$ . Since all integral powers of  $-1$  are  $\pm 1$ , the congruence is equivalent to the equality  $(-1/p) = (-1)^{(p-1)/2}$ .

The following theorem, which gives a method for finding all quadratic residues of a given odd prime modulus, may be proved using the properties of Legendre's symbol.

Theorem 5. The integers

$$(15) \quad 1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$$

are incongruent quadratic residues of the odd prime  $p$ .

Proof. By property III of theorem 7, each of the integers in the sequence (16) is a quadratic residue of  $p$ ; and because  $c^2 \equiv (p-c)^2 \pmod{p}$ , only those integers are necessary to determine the quadratic residues modulo  $p$ . Moreover, no two of the integers are congruent modulo  $p$  because  $c_i^2 \equiv c_j^2 \pmod{p}$  implies  $(c_i - c_j)(c_i + c_j) \equiv 0 \pmod{p}$ , which implies that  $p$  divides at least one of the factors  $c_i - c_j$  and  $c_i + c_j$ . Since both  $c_i$  and  $c_j$  are positive and distinct elements not greater than  $(p-1)/2$ , neither  $c_i - c_j$  nor  $c_i + c_j$  is divisible by  $p$ . From the integers of the set (16) all quadratic residues of  $p$  may be found.

Thus far, quadratic residues have been considered only in regard to the question of the existence of solutions, that is, determining the quadratic character of a number for a given odd prime modulus. However, the theory of quadratic residues centered around Legendre's symbol is of greater scope. The Legendre symbol allows both determining the quadratic character of an integer modulo  $p$  and finding the primes  $p$  of which a particular integer is a quadratic residue.

The latter problem is now considered. Property V of theorem 7 shows  $-1$  to be a quadratic residue for all primes  $p$ . The following theorem gives the odd primes for which  $-1$  is a quadratic residue.

Theorem 9. The integer  $-1$  is a quadratic residue of all primes of the form  $4n+1$  and a quadratic non-residue of all primes of the form  $4n+3$ .

Proof. The proof is divided into two cases.

Case I: Since  $(p-1)/2$  is even for  $p \equiv 1 \pmod{4}$ , from property VI of theorem 7,  $(-1/p) = +1$ . Hence,  $-1$  is a quadratic residue of  $p = 4n+1$ .

Case II: Since  $(p-1)/2$  is odd for  $p \equiv 3 \pmod{4}$ , from property VI of theorem 7,  $(-1/p) = -1$ . Hence,  $-1$  is a quadratic non-residue of  $p = 4n+3$ .

The following theorem, attributed to Gauss, gives a method for finding the primes  $p$  of which any integer  $q$ , not a multiple of  $p$ , is a quadratic residue.

Theorem 10. (Gauss's lemma) Let  $p$  be any odd prime such that  $p$  does not divide  $q$ . If  $v$  is the number of elements of the set

$$(17) \quad q, 2q, 3q, \dots, \frac{(p-1)q}{2}$$

whose numerically least residues modulo  $p$  are negative, then

$$(q/p) = (-1)^v.$$

Proof. The integers of the set (17) are prime to  $p$  and incongruent modulo  $p$ . Their numerically least residues modulo  $p$  are

$a_1, a_2, \dots, a_u$  representing the positive ones and  $-b_1, -b_2, \dots, -b_v$

representing the negative ones. Since the integers (17) are incongruent modulo  $p$ , no two  $a_i$ 's are equal and no two  $b_j$ 's are equal. Since both

$a_i$  and  $-b_j$  are congruent modulo  $p$  to integers of (17), they may be

denoted by  $a_i \equiv sq \pmod{p}$  and  $-b_j \equiv tq \pmod{p}$ , where  $s$  and  $t$  are integers

of the set  $1, 2, \dots, (p-1)/2$ . Assuming  $a_i \equiv b_j \pmod{p}$  for some  $i$  and  $j$ ,

leads to a contradiction because it implies  $a_i - b_j \equiv 0 \pmod{p}$  which

implies  $(s-t)q \equiv 0 \pmod{p}$  since  $q \not\equiv 0 \pmod{p}$ . Since  $s$  and  $t$  are both

positive integers less than  $(p-1)/2$ , the sum cannot be a multiple of  $p$ ;

hence, the  $(p-1)/2$  numbers  $a_1, a_2, \dots, a_u, b_1, b_2, \dots, b_v$  are distinct

integers between 1 and  $(p-1)/2$ . They are therefore exactly the numbers 1, 2, . . . ,  $(p-1)/2$  in some order. The product of the original set of integers (17) is congruent modulo  $p$  to the product

$$(18) \quad (-1)^V a_1 a_2 a_3 \dots a_u b_1 b_2 \dots b_v.$$

Now the product of the set (17) may be written  $q^{(p-1)/2} (p-1)!$ ,

and (18) may be written  $(-1)^V (p-1)!$ . Therefore,  $q^{(p-1)/2} \equiv (-1)^V \pmod{p}$ .

From Euler's criterion this becomes  $(q/p) \equiv (-1)^V \pmod{p}$ . Since both members of the congruence may assume only values  $\pm 1$ , the equality to be proved follows; that is,  $(q/p) = (-1)^V$ .

The next theorem to be proved is an extension of Gauss's lemma giving the quadratic character of primes for all odd primes. However, a lemma defining the use of the bracket function must first be proved. The theorem then follows.

Lemma. When  $k$  and  $p$  are positive integers, the division of  $k$  by  $p$  to give a non-negative remainder,  $r < p$ , yields the quotient  $[k/p]$ . That is,  $k = p[k/p] + r$ ,  $0 \leq r < p$ .

Proof. By the division algorithm, given any two positive integers  $k$  and  $p$ , there exist integers  $Q$  and  $r$  such that  $k = pQ + r$ ,  $0 \leq r < p$ .

Thus,  $k/p = Q + r/p$ ,  $0 \leq r/p < 1$ . Hence,  $Q$  is the integral part and  $r/p$  is the decimal part of  $k/p$ . Since the bracket function  $[x]$  is defined to be the greatest integer less than or equal to  $x$ ,  $Q = [k/p]$ .

Substituting this into the original expression for  $k$  gives the equation to be proved.

Theorem 11. If  $p$  is an odd prime, then for an odd prime  $q \neq p$ ,

$$(q/p) = (-1)^{ii} \text{ with}$$

$$(19) \quad H = \left[ \frac{a}{p} \right] + \left[ \frac{2a}{p} \right] + \dots + \left[ \frac{ta}{p} \right]$$

in which  $t = (p-1)/2$ ; and for  $q = 2$ ,  $(a/p) = (-1)^{(p^2-1)/8}$ .

Proof. If  $q$  is any prime not equal to  $p$ , the lemma applies to each of the multiples of  $q$  given in (17). If their least residues are denoted by  $r_1, r_2, \dots, r_t$  with  $0 \leq r_k < p$

the numbers in (17) are given by the lemma as follows:

$$\begin{aligned} q &= p \left[ \frac{q}{p} \right] + r_1 \\ (20) \quad 2q &= p \left[ \frac{2q}{p} \right] + r_2 \\ &\dots \\ tq &= p \left[ \frac{tq}{p} \right] + r_t. \end{aligned}$$

If  $H$  is the sum given in (19) and  $S$  is the sum of the first  $(p-1)/2$  positive integers, adding the equations (20) yields

$$(21) \quad Sq = p \cdot t + \sum_{k=1}^t r_k.$$

The numerically least residues were denoted in theorem 10 by  $a_i$  and  $-b_j$ ,  $i = 1, 2, \dots, u$ ,  $j = 1, 2, \dots, v$ . The  $-b_j$ 's are the negatively least residues. However, since  $-b_j \equiv p - b_j \pmod{p}$  and  $0 \leq p - b_j < p$ , all  $r_k$ 's are given by all  $a_i$ 's and all  $(p - b_j)$ 's together. Denoting

$\sum_{i=1}^u a_i = A$  and  $\sum_{j=1}^v b_j = B$ , equation (21) becomes

$$(22) \quad Sq = p \cdot t + v \cdot p - B$$

As was noted in the proof of theorem 10,

$$(23) \quad S = A + B.$$

Subtracting equation (23) from equation (22) yields  $(q-1)S = pM + vp - 2B$ , which is equivalent to

$$(24) \quad (q-1)S \equiv p(M+vp) \pmod{2}.$$

Since the sum of the first  $(p-1)/2$  positive integers equals  $(p^2-1)/8$ , (24) becomes

$$(25) \quad (q-1)(p^2-1)/8 \equiv p(M+vp) \pmod{2}.$$

In conclusion, two cases arise.

Case I: If  $q$  is odd, congruence (25) becomes  $p(n+vp) \equiv 0 \pmod{2}$ .

Therefore, since  $p$  is an odd prime,  $M \equiv -v \pmod{2}$ . Since  $-v \equiv v \pmod{2}$ ,  $M \equiv v \pmod{2}$ . Then Gauss's lemma for any odd prime  $q$  becomes  $(q/p) = (-1)^M$ .

Case II: If  $q=2$ , each of the bracket functions of  $M$  is some  $[d]$ ; but  $d$  is in each case less than one. Therefore,  $M = 0$ . Then congruence (25) becomes  $(p^2-1)/8 \equiv pv \pmod{2}$ . Because  $p$  is an odd prime  $pv \equiv v \pmod{2}$ , then  $(p^2-1)/8 \equiv v \pmod{2}$ . Gauss's lemma for  $q=2$  is then equivalent to  $(2/p) = (-1)^{(p^2-1)/8}$ .

The following is an example of the use of the preceding results and the properties of Legendre's symbol.

Example 2. Find all odd primes for which  $-2$  is a quadratic residue. Evaluating  $(-2/p)$  yields

$$(-2/p) = (-1/p)(2/p) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8} = (-1)^{(p-1)/2 + (p^2-1)/8}.$$

Those odd primes which give an even exponent are of the forms  $8n+1$  and  $8n+3$ . Those giving an odd exponent are of the forms  $8n-1$  and  $8n-3$ .

Therefore, of the four distinct classes of odd primes modulo 8,  $-2$  is a residue of  $p = 1 \pmod{8}$  and  $p = 3 \pmod{8}$ . Then,  $-2$  is a non-residue of  $p = 5 \pmod{8}$  and  $p = 7 \pmod{8}$ .

## THE LAW OF QUADRATIC RECIPROCITY

Finally with the preceding results, one is able to consider the famous law of quadratic reciprocity. This theorem was discovered at different times by Euler (1783), by Legendre (1785), and finally by Gauss (1795), who found a total of seven different proofs for the theorem. The proof given here is the fifth proof of Gauss, based on his lemma, a transformation of Euler's criterion.<sup>6</sup>

Theorem 12. (Law of Quadratic Reciprocity) For any two distinct odd primes  $p$  and  $q$ ,  $(q/p)(p/q) = (-1)^{(p-1)/2 \cdot (q-1)/2}$  which is equivalent to  $(q/p) = (-1)^{(p-1)/2 \cdot (q-1)/2} (p/q)$ .

Proof. By Gauss's lemma  $(q/p) = (-1)^u$  and  $(p/q) = (-1)^v$  if  $u$  and  $v$  are the numbers of the multiples  $q, 2q, \dots, \frac{p-1}{2}q$  and  $p, 2p, \dots, \frac{q-1}{2}p$  having negative numerically least residues modulo  $p$  and modulo  $q$  respectively. Since Gauss's lemma gives  $(q/p)(p/q) = (-1)^{u+v}$ , it suffices to show that  $(u+v)$  and  $(p-1)/2 \cdot (q-1)/2$  are of the same parity--in congruence notation,  $u+v \equiv (p-1)/2 \cdot (q-1)/2 \pmod{2}$ .

The least positive residue of any number modulo  $pq$  either is zero or belongs to the series

$$(26) \quad 1, 2, 3, \dots, pq-1.$$

This series is composed of the two series

$$(27) \quad 1, 2, \dots, (pq-1)/2$$

$$(28) \quad (pq+1)/2, (pq+3)/2, \dots, pq-1.$$

Each of the numbers of (27), none of which are divisible by  $pq$ , may

---

<sup>6</sup>J. V. Uspensky and M. A. Heaslet, Elementary Number Theory, pp. 284-6.

be characterized by the combination of both its modulo  $p$  and its modulo  $q$  numerically least residues. All eight different possible combinations are listed although classes 1, 6, and 8 will not be needed for the proof of the theorem.

Class 1 contains numbers with numerically least residues positive modulo  $p$  and positive modulo  $q$ . Let  $e$  of the numbers of (27) be of this type.

Class 2 contains numbers with numerically least residues positive modulo  $p$  and negative modulo  $q$ . Let  $f$  of the numbers of (27) be of this type.

Class 3 contains numbers with numerically least residues negative modulo  $p$  and positive modulo  $q$ . Let  $g$  of the numbers of (27) be of this type.

Class 4 contains numbers with numerically least residues negative modulo  $p$  and negative modulo  $q$ . Let  $h$  of the numbers of (27) be of this type.

Class 5 contains all multiples of  $q$  with numerically least residues negative modulo  $p$ . All multiples of  $q$  in (27) are  $q, 2q, \dots, \frac{p-1}{2}q$ . Consequently, class 5 contains  $u$  numbers.

Class 6 contains all multiples of  $q$  with numerically least residues positive modulo  $p$ . Their number is  $(p-1)/2 - u$ .

Class 7 contains all multiples of  $p$  with numerically least residues negative modulo  $q$ . All multiples of  $p$  in (27) are  $p, 2p, \dots, \frac{q-1}{2}p$ . Consequently, class 7 contains  $v$  numbers.

Class 8 contains all multiples of  $p$  with numerically least residues positive modulo  $q$ . Their number is  $(q-1)/2 - v$ .

Classes 2, 4, and 7 comprise all numbers of the set (27) having negative numerically least residues modulo  $q$ . For a given least residue  $r_1$ , negative modulo  $q$ , the numbers of (27) with least residue  $r_1$ , are  $qr_1, 2qr_1, \dots, \frac{p-1}{2}qr_1$ . Hence, for a particular  $r_1$ , the set (27) is composed of  $(p-1)/2$  numbers. But  $r_1$  can be any one of  $(q-1)/2$  different values. Therefore, the number of integers of (27) having negative numerically least residues modulo  $q$  is  $(p-1)/2 \cdot (q-1)/2$ . This is also the number of integers in classes 2, 4, and 7, so that

$$(29) \quad f+h+v = (p-1)/2 \cdot (q-1)/2.$$

By similar enumeration, interchanging the roles of  $p$  and  $q$  and considering classes 3, 4, and 5, one obtains

$$(30) \quad g+h+u = (p-1)/2 \cdot (q-1)/2.$$

To each number  $c$  in (27) with numerically least residue negative modulo  $p$  and positive modulo  $q$  there corresponds a number  $pq-c$  in (26) with numerically least residue positive modulo  $p$  and negative modulo  $q$ . Since this is a one-to-one correspondence, there are exactly as many integers in class 3 as there are integers in (28) having numerically least residues positive modulo  $p$  and negative modulo  $q$ . Since the integers in (27) having numerically least residues positive modulo  $p$  and negative modulo  $q$  are those of class 2, the number of integers of (26) with numerically least residues positive modulo  $p$  and negative modulo  $q$  is the sum of the number of integers in classes 2 and 3,  $f+g$ . Those integers of (26) are of the form  $k_1p+k_2q$  for which  $k_1p$  is a negative numerically least residue modulo  $q$  and  $k_2q$  is a positive numerically least residue modulo  $p$ . Since  $k_1p$  ranges over  $(q-1)/2$

distinct values and  $k_2 q$  ranges over  $(p-1)/2$  distinct values, the number of integers of (26) with numerically least residues positive modulo  $p$  and negative modulo  $q$  is  $(p-1)/2 \cdot (q-1)/2$ . Therefore,

$$(31) \quad f + g = (p-1)/2 \cdot (q-1)/2.$$

Equation (31) subtracted from the sum of equations (29) and (30) results in  $u+v+2h = (p-1)/2 \cdot (q-1)/2$ . Hence  $u+v \equiv (p-1)/2 \cdot (q-1)/2 \pmod{2}$ , which was to be proved, yielding

$$(32) \quad (q/p)(p/q) = (-1)^{(p-1)/2 \cdot (q-1)/2}.$$

Since  $(p/q)$  is  $+1$  or  $-1$ , multiplying both sides of equation (32) by  $(p/q)$  gives

$$(33) \quad (q/p) = (-1)^{(p-1)/2 \cdot (q-1)/2} (p/q).$$

The following is an example of an application of the law of quadratic reciprocity.

Example 3. Find the primes of which 3 is a quadratic residue.

Equation (33) with  $a = 3$  is  $(3/p) = (-1)^{(p-1)/2} (p/3)$ . If

$p \equiv 1 \pmod{4}$ ,  $(-1)^{(p-1)/2} = +1$ . If  $p \equiv 3 \pmod{4}$ ,  $(-1)^{(p-1)/2} = -1$ .

For  $p \equiv 1 \pmod{3}$ ,  $(p/3) = +1$ . For  $p \equiv 2 \pmod{3}$ ,  $(p/3) = (-1)^{(p-1)/3} = -1$ .

Since  $(3/p)$  equals  $+1$  if and only if  $(p/3)$  and  $(-1)^{(p-1)/2}$  are of the same sign, 3 is a quadratic residue of primes of the form  $p \equiv 1 \pmod{12}$  and  $p \equiv 11 \pmod{12}$ .

#### THE JACOBI SYMBOL

For composite numbers  $q$  the solution of problems of the type in example 3 requires consideration of cases according to the quadratic character of the prime factors of  $q$ . This is simplified by the use of

a generalization of Legendre's symbol, known as the Jacobi symbol. If  $P = p_1 p_2 \dots p_k$  and the  $p_i$  with  $i = 1, 2, \dots, k$  are positive, odd primes not necessarily distinct, then for any integer  $c$  relatively prime to  $P$  the Jacobi symbol  $(c/P)$  is defined as follows:  
 $(c/P) = (c/p_1)(c/p_2) \dots (c/p_k)$ , interpreting the symbols to the right of the equality sign as Legendre symbols.

The following theorem gives properties of the Jacobi symbol similar to those of the Legendre symbol given in theorem 7. The letters,  $P$  and  $P'$ , denote products of positive, odd primes relatively prime to the integers  $c$  and  $b$ .

Theorem 12. The Jacobi symbol has the following properties;

- I.  $(c/PP') = (c/P)(c/P')$
- II.  $(cb/P) = (c/P)(b/P)$
- III. If  $c \equiv b \pmod{P}$ , then  $(c/P) = (b/P)$ .
- IV.  $(c^2/P) = (c/P^2) = 1$
- V.  $(cb^2/P'P^2) = (c/P')$

Proof. Each of the five properties must be considered separately.

Property I. This property is a direct application of the definition of the Jacobi symbol.

Property II. If this is written in terms of Legendre's symbols by definition,  $\prod_{i=1}^k (cb/p_i) = \prod_{i=1}^k (c/p_i) \prod_{i=1}^k (b/p_i)$ , and if terms to the right of the equality sign are rearranged,  $\prod_{i=1}^k (cb/p_i) = \prod_{i=1}^k (c/p_i)(b/p_i)$ , which is verified by property I of theorem 7 for each  $i=1, 2, \dots, k$ .

Property III. Again  $P$  may be written  $p_1 p_2 \dots p_k$ . Then  $c \equiv b \pmod{p_1}$ .

Hence,  $(c/p_1) = (b/p_1)$  by property II of theorem 7. Application of this property for  $i=1, 2, \dots, k$  and multiplication yields  $\prod_{i=1}^k (c/p_i) = \prod_{i=1}^k (b/p_i)$ ,

which is by definition property III as given.

Property IV. By properties I and II respectively, both  $(c/P^2)$  and

$(c^2/P)$  are equivalent to  $(c/P)(c/P)$ . The Jacobi symbol  $(c/P)$ , product of Legendre symbols, has the value  $+1$  or  $-1$ . In either case,  $(c/P)(c/P) = +1$ .

Property V. The reduction of the left side of this equation to the right side using properties I, II and IV is as follows:

$$(cb^2/P^2) = (cb^2/P')(cb^2/P^2) = (cb^2/P') = (c/P')(b^2/P') = (c/P').$$

The next two theorems give the value of the Jacobi symbol for  $c = -1$  and for  $c = 2$ .

Theorem 14. For any odd integer  $P > 1$ ,  $(-1/P) = (-1)^{(P-1)/2}$ .

Proof. For odd integers  $p_1$  and  $p_2$ ,  $(p_1-1)(p_2-1) \equiv 0 \pmod{4}$ . Then

$p_1 p_2 - p_1 - p_2 + 1 \equiv 0 \pmod{4}$ , which is equivalent to

$$p_1 p_2 - 1 \equiv (p_1 - 1) + (p_2 - 1) \pmod{4} \text{ or } (p_1 p_2 - 1)/2 \equiv (p_1 - 1)/2 + (p_2 - 1)/2 \pmod{2}.$$

If this is extended to odd integers  $p_1, p_2, \dots, p_k$ , then

$$(34) \quad \sum_{i=1}^k (p_i - 1)/2 = (\prod_{i=1}^k p_i - 1)/2 \pmod{2}.$$

By definition  $(-1/P) = \prod_{i=1}^k (-1/p_i)$ , which by property VI of theorem 7 is

$$(-1/P) = \prod_{i=1}^k (-1)^{(p_i-1)/2}. \text{ The law of exponents for multiplication then}$$

gives  $(-1/P) = (-1)^{\sum_{i=1}^k (p_i-1)/2}$ , which by (34) is  $(-1/P) = (-1)^{\sum_{i=1}^k (p_i-1)/2}$ .

Hence,  $(-1/P) = (-1)^{(P-1)/2}$ .

Theorem 15. For any odd integer  $P > 1$ ,  $(2/P) = (-1)^{(P^2-1)/8}$ .

Proof. For odd integers  $p_1$  and  $p_2$ ,  $(p_1^2-1)(p_2^2-1) \equiv 0 \pmod{16}$ .

Then  $p_1^2 p_2^2 - 1 \equiv (p_1^2-1) + (p_2^2-1) \pmod{16}$ , or

$(p_1^2 p_2^2 - 1)/8 \equiv (p_1^2-1)/8 + (p_2^2-1)/8 \pmod{2}$ . For odd integers

$p_1, p_2, \dots, p_k$ ,

$$(35) \quad \left( \prod_{i=1}^k p_i^2 - 1 \right) / 8 \equiv \sum_{i=1}^k (p_i^2 - 1) / 8 \pmod{2}.$$

By reasoning similar to that of the proof of theorem 14, using case II

of theorem 11 and equation (35),  $(2/P) = \prod_{i=1}^k (2/p_i) = \prod_{i=1}^k (-1)^{(p_i^2-1)/8}$   
 $= (-1)^{\sum_{i=1}^k (p_i^2-1)/8} = (-1)^{(\prod_{i=1}^k p_i^2 - 1)/8}$ . Hence,  $(2/P) = (-1)^{(P^2-1)/8}$ .

#### THE GENERALIZED LAW OF QUADRATIC RECIPROCITY

The following theorem is a generalization of the law of quadratic reciprocity to deal with the Jacobi symbol.

Theorem 16. For odd integers  $P, Q > 1$ ,  $(P/Q)(Q/P) = (-1)^{(P-1)/2 \cdot (Q-1)/2}$

which is equivalent to  $(Q/P) = (-1)^{(P-1)/2 \cdot (Q-1)/2} (P/Q)$ .

Proof. If  $P$  and  $Q$  can be decomposed into prime factors,  $P = \prod_{i=1}^s p_i$

and  $\epsilon = \prod_{j=1}^t q_j$ , then by properties I and II of theorem 13,

$$(P/Q) = \left( \prod_{i=1}^s p_i / \prod_{j=1}^t q_j \right) = \prod_{i=1}^s (p_i / \prod_{j=1}^t q_j) = \prod_{i=1}^s \prod_{j=1}^t (p_i / q_j). \text{ Similarly,}$$

$$(Q/P) = \prod_{j=1}^t \prod_{i=1}^s (q_j / p_i). \text{ Therefore, } (P/Q)(Q/P) = \prod_{i=1}^s \prod_{j=1}^t (p_i / q_j)(q_j / p_i),$$

which by the quadratic reciprocity law is equivalent to

$$\prod_{i=1}^s \prod_{j=1}^t (-1)^{(p_i-1)/2 \cdot (q_j-1)/2}. \text{ Then using an argument similar to that}$$

of theorem 14, one obtains

$$(P/Q)(Q/P) = (-1)^{(\prod_{i=1}^s p_i - 1)/2 \cdot (\prod_{j=1}^t q_j - 1)/2}. \text{ Hence,}$$

$(P/Q)(Q/P) = (-1)^{(P-1)/2 \cdot (Q-1)/2}$ . Since  $(P/Q)$  is  $+1$  or  $-1$ , multiplying both sides of the preceding equation by  $(P/Q)$  yields

$$(Q/P) = (-1)^{(P-1)/2 \cdot (Q-1)/2} (P/Q).$$

According to the definition of the Jacobi symbol,  $(c/p)$  is  $+1$  when all  $(c/p_i) = +1$  or when an even number are  $-1$ . In the first case each of the congruences

$$(36) \quad x^2 \equiv c \pmod{p_i} \text{ for } i = 1, 2, \dots, k$$

has a solution; hence, there is a solution of

$$(37) \quad x^2 \equiv c \pmod{P}.$$

In the second case, however, some of the congruences (36) fail to have a solution; therefore, congruence (37) has no solution. The Jacobi symbol does not have the direct connection with quadratic residues that the Legendre symbol has; that is,  $(c/P) = +1$  is a necessary but

not a sufficient condition that  $c$  be a quadratic residue of  $P$ . However,  $(c/P) = -1$  is obviously a sufficient condition that  $c$  be a quadratic non-residue of  $P$ .

Jacobi symbols can be used in evaluating Legendre symbols and shorten considerably the computations required. The reciprocity law for the Legendre symbol requires that the two integers both be odd primes. Thus it is necessary in evaluating the symbol  $(c/p)$  to factor  $c$  into prime factors and to consider the product of Legendre symbols involving only primes, using the quadratic reciprocity law to evaluate each. On the other hand, if the symbol  $(c/p)$  is interpreted as a Jacobi symbol, the only factorization necessary is of the form

$$(38) \quad (c/p) = (-1/p)^s (2/p)^t (b/p) \text{ with } s, t = 0,$$

to obtain  $b$  odd and positive, but not necessarily prime. The values of  $(-1/p)^s$  and  $(2/p)^t$  are computed directly and the value of  $(b/p)$  is obtained using the law of quadratic reciprocity for Jacobi symbols.

The following example illustrates in part I the use of only Legendre symbols; for comparison, part II illustrates the use of the Jacobi symbol to solve the same problem.

Example 4. Determine whether or not the following congruence has a solution:

$$(39) \quad x^2 \equiv -35 \pmod{71}.$$

Since 71 is a prime,  $(-35/71)$  may be interpreted as either Legendre's symbol or Jacobi's symbol.

Part I: In order to use the reciprocity law for Legendre symbols, the symbol must involve two distinct odd primes. Hence,

$(-35/71) = (-1/71)(5/71)(7/71)$ . By property VI of theorem 7,

$(-1/71) = (-1)^{(71-1)/2} = (-1)^{35} = -1$ . Using the law of quadratic

reciprocity since both 5 and 71 are odd primes,  $(5/71)(71/5) = (-1)^{35 \cdot 2} = +1$ ;

and  $(71/5) = (1/5) = +1$ . Therefore,  $(5/71) = +1$ . Since both 7 and 71 are odd primes, the law of quadratic reciprocity is used, yielding

$(7/71)(71/7) = (-1)^{3 \cdot 35} = -1$ . Then, since  $(71/7) = (1/7) = +1$ ,  $(7/71) = -1$ .

Hence,  $(-35/71) = (-1)(+1)(-1) = +1$ ; therefore,  $-35$  is a quadratic residue of 71. Congruence (39) does have a solution.

Part II: The reciprocity law for Jacobi symbols requires the factorization (38). Hence,  $(-35/71) = (-1/71)(35/71)$ . As it was obtained in part I,  $(-1/71) = -1$ . Using the law of quadratic reciprocity for Jacobi

symbols,  $(35/71)(71/35) = (-1)^{34/2 \cdot 70/2} = (-1)^{17 \cdot 35} = -1$ . Now,

$(71/35) = (1/35) = +1$ ; therefore,  $(35/71) = -1$ . Since 71 is a prime,

there are no factors  $(c/p_1)$  to consider. Hence,  $(-35/71) = (-1)(-1) = +1$ .

This indicates that  $-35$  is a quadratic residue of 71.

#### CONCLUSION

Finally, the problem of solving quadratic congruences is considered in light of the results of this investigation of the theory of quadratic residues. A final example to illustrate the use of these results is given.

Example 5. Solve the quadratic congruences  $f(x) \equiv 0 \pmod{35}$  in which

$$(40) \quad f(x) = 4x^2 + 2x + 1.$$

Because the modulus of the congruence is a composite integer the first

step in the problem is to factor  $35 = 7 \cdot 5$ . Then the solutions of both  $f(x) \equiv 0 \pmod{7}$  and  $f(x) \equiv 0 \pmod{5}$  are needed to use the Chinese method to find all solutions of  $f(x) \equiv 0 \pmod{35}$ . Thus the problem separates into two parts.

Part I. Since for  $f(x) \equiv 0 \pmod{7}$  the modulus is an odd prime, theorem 4 applies to the problem giving the following two congruences to solve:

$$(41) \quad 8x + 2 \equiv u \pmod{7}$$

$$(42) \quad u^2 \equiv -12 \pmod{7}.$$

Congruence (42) reduces to

$$(43) \quad u^2 \equiv 2 \pmod{7};$$

then the quadratic character of 2 with respect to 7 is needed to ascertain the existence of solutions of (43). Theorem 11 for  $q = 2$  yields  $(2/7) = (-1)^{(49-1)/8} = (-1)^6 = +1$ . Hence 2 is a quadratic residue of 7; by theorem 5, (43) has two solutions. By trial of integers modulo 7,  $3^2 = 9 \equiv 2 \pmod{7}$ . Hence, the two solutions are  $u \equiv \pm 3 \pmod{7}$ , that is, 3 or 4 (mod 7). Congruence (41) is then used to find values of  $x$  satisfying  $f(x) \equiv 0 \pmod{7}$ . For  $u \equiv 3 \pmod{7}$ ,  $8x + 2 \equiv 3 \pmod{7}$ ;  $x \equiv 1 \pmod{7}$ . For  $u \equiv 4 \pmod{7}$ ,  $8x + 2 \equiv 4 \pmod{7}$ ;  $x \equiv 2 \pmod{7}$ . Therefore, the two solutions of  $f(x) \equiv 0 \pmod{7}$  are 1 and 2.

Part II. Since for  $f(x) \equiv 0 \pmod{5}$  the modulus is an odd prime, theorem 4 applies, giving the congruences

$$(44) \quad 8x + 2 \equiv u \pmod{5}$$

$$(45) \quad u^2 \equiv -12 \pmod{5}.$$

Congruence (45) reduces to

$$(46) \quad u^2 \equiv 3 \pmod{5};$$

then the quadratic character of 3 with respect to 5 is needed. Since 3 and 5 are both odd primes, the law of quadratic reciprocity applies to the problem of evaluating the Legendre symbol as follows:

$(3/5)(5/3) = (-1)^{(5-1)/2 \cdot (3-1)/2} = (-1)^2 = +1$ . Now  $(5/3) = (2/3) = (-1)^{(3-1)/2} = -1$ . Therefore,  $(3/5) = -1$ . Then 3 is a quadratic non-residue of 5, and (46) has no solution. Furthermore,  $f(x) \equiv 0 \pmod{5}$  has no solution; hence,  $f(x) \equiv 0 \pmod{35}$  fails to have a solution.

This example illustrates the dependence of a quadratic congruence with composite modulus upon congruences with prime moduli which in turn depend upon the respective binomial congruences. It indicates the value of the theory of quadratic residues, which allows one to determine the number of solutions. The greatest advantage is in determining that no solution exists without the trial substitution of all integers of the modulo system to find that none satisfy the congruence. On the other hand, if solutions of (46) had been found, the corresponding solutions of (44) would have been determined as was done in part I. These would have been the solutions of  $f(x) \equiv 0 \pmod{5}$ . Then the Chinese method, as in example 1, would have given all solutions of  $f(x) \equiv 0 \pmod{35}$  from the two congruences modulo 5 and modulo 7.

#### ACKNOWLEDGMENT

The writer wishes to thank Professor Richard L. Yates for his careful reading of this paper in its early form and for his subsequent advice and aid in preparation of the final copy.

#### BIBLIOGRAPHY

- Dickson, Leonard Eugene. Modern Elementary Theory of Numbers. Chicago: The University of Chicago Press, 1939.
- Griffin, Harriet. Elementary Theory of Numbers. New York: McGraw-Hill Book Company, Inc., 1954.
- Landau, Edmund. Elementary Number Theory. New York: Chelsea Publishing Company, 1958.
- LeVeque, William Judson. Topics in Number Theory. 2 vols. Reading, Mass.: Addison-Wesley Publishing Company, Inc., 1956.
- Niven, Ivan and Zuckerman, Herbert S. An Introduction to the Theory of Numbers. New York: John Wiley and Sons, Inc., 1960.
- Stewart, Bonnie M. Theory of Numbers. New York: The Macmillan Company, 1952.
- Uspensky, J. V. and Heaslet, M. A. Elementary Number Theory. New York: McGraw-Hill Book Company, Inc., 1939.
- Wright, Harry N. First Course in Theory of Numbers. New York: John Wiley and Sons, Inc., 1939.

QUADRATIC CONGRUENCES

by

MARY JEANE STARKEY MCGUIRE

B. A., Kansas State University, 1961

---

AN ABSTRACT OF  
A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY  
Manhattan, Kansas

1963

A given quadratic congruence,  $f(x) \equiv 0 \pmod{m}$  can be solved by trial substitution of one integer from each of the  $m$  equivalence classes to find all solutions of the congruence. For  $m = 2$  the two representatives 0 and 1 may readily be tried. Obviously, there can be at most two solutions. By Lagrange's theorem there are also at most two solutions of the quadratic congruence if  $m$  is an odd prime. If  $m$  is an odd prime, the solutions of the quadratic congruence are equivalent to the solutions of a corresponding pair of congruences--a linear and a binomial quadratic congruence. Solutions of the binomial quadratic congruence are substituted into the linear congruence to give solutions of the original quadratic congruence of odd prime modulus. If  $m$  is some positive power  $s$  of a prime  $p$ , the quadratic congruence modulo  $p$  is first solved. Each of these solutions--at most two--determines either 0, 1, or  $p$  solutions of the congruence modulo  $p^2$ ; and to each thus obtained there will correspond 0, 1, or  $p$  solutions of the congruence modulo  $p^3$ . The process is continued through successive powers of  $p$  to the congruence modulo  $p^s$ . The existence of solutions modulo  $p$  is a necessary but not a sufficient condition for the existence of solutions modulo  $p^s$ . If  $m$  is a product of positive powers of primes, that is  $m = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r}$ , the Chinese method is used to solve the system of congruences obtained from all solutions of the  $r$  different quadratic congruences modulo  $p_i^{s_i}$  for  $i = 1, 2, \dots, r$ . The number of these solutions is the product of the numbers of solutions of each congruence modulo  $p_i^{s_i}$  with  $i = 1, 2, \dots, r$ .

Hence, solving quadratic congruences reduces to solving first the corresponding binomial quadratic congruence. The question of the existence of solutions of the binomial quadratic congruence is basic to the theory of quadratic residues. Legendre's symbol is the fundamental tool by which existence of such solutions may be determined. The law of quadratic reciprocity allows evaluation of the Legendre symbol,  $(q/p)$ , for odd primes  $q$  and  $p$ . The generalized quadratic reciprocity law, for the Jacobi symbol, allows computations without the restriction on  $q$  and  $p$ . However, the theory of quadratic residues gives only the number of solutions that exist for a binomial quadratic congruence with odd prime modulus. Solutions are found by trial substitution. The practical value of the existence theory lies in being able to ascertain that no solutions exist without making  $m$  trial substitutions.